AF
JFW

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application No.	09/965, 579
Filing Date	September 26, 2001
First Named Inventor	Linden Minnick
Art Unit	2137
Examiner Name	Michael J. Pyzocha
Total Number of Pages in This Submission	17
Attorney Docket Number	42390P12266

ENCLOSURES ***(check all that apply)***

- [X] Fee Transmittal Form
  - [X] Fee Attached
- [ ] Amendment / Response
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
  - [ ] PTO/SB/08
- [ ] Certified Copy of Priority Document(s)
- [ ] Response to Missing Parts/ Incomplete Application
  - [ ] Basic Filing Fee
  - [ ] Declaration/POA
  - [ ] Response to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s)
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [X] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [X] Other Enclosure(s) *(please identify below):*

* Check for $500
* Return Receipt Postcard

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Vincent H. Anderson, Reg. No. 54,962 BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Signature	
Date	February 28, 2006

CERTIFICATE OF MAILING/TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Typed or printed name	Theresa Belland		
Signature		Date	February 28, 2006

Based on PTO/SB/21 (09-04) as modified by Blakely, Solokoff, Taylor & Zafman (wlr) 11/30/2005.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

FEE TRANSMITTAL for FY 2005

Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27.

TOTAL AMOUNT OF PAYMENT ($) 500.00

Complete if Known	
Application Number	09/965, 579
Filing Date	September 26, 2001
First Named Inventor	Linden Minnick
Examiner Name	Michael J. Pyzocha
Art Unit	2137
Attorney Docket No.	42390P12266

METHOD OF PAYMENT *(check all that apply)*

☒ Check ☐ Credit card ☐ Money Order ☐ None ☐ Other (please identify): _____

☒ Deposit Account Deposit Account Number: 02-2666 Deposit Account Name: Blakely, Sokoloff, Taylor & Zafman LLP

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☐ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, except for the filing fee

☒ Charge any additional fee(s) or underpayment of fee(s) under 37 CFR §§ 1.16, 1.17, 1.18 and 1.20. ☒ Credit any overpayments

FEE CALCULATION

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet.	
2053	130	2053	130	Non-English specification	
1251	120	2251	60	Extension for reply within first month	
1252	450	2252	225	Extension for reply within second month	
1253	1,020	2253	510	Extension for reply within third month	
1254	1,590	2254	795	Extension for reply within fourth month	
1255	2,160	2255	1,080	Extension for reply within fifth month	
1401	500	2401	250	Notice of Appeal	
1402	500	2402	250	Filing a brief in support of an appeal	500.00
1403	1,000	2403	500	Request for oral hearing	
1451	1,510	2451	1,510	Petition to institute a public use proceeding	
1460	130	2460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
1809	790	1809	395	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	790	2810	395	For each additional invention to be examined (37 CFR § 1.129(b))	

Other fee (specify) _____

SUBTOTAL (2) ($) 500.00

SUBMITTED BY Complete (if applicable)

Name (Print/Type)	Vincent H. Anderson	Registration No. (Attorney/Agent)	54,962	Telephone	(503) 439-8778
Signature				Date	02/28/06

Based on PTO/SB/17 (12-04) as modified by Blakely, Sokoloff, Taylor & Zafman (wlr) 12/15/2004.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS

In re application of: **Minnick**	Examiner: Michael J. Pyzocha
Application No: 09/965,579	Art Unit: 2137
Filed: September 26, 2001	
For: SECURITY ASSOCIATION MANAGEMENT THROUGH THE USE OF LOOKUP TABLES	

Mail Stop Appeal Brief-Patents
Assistant Commissioner For Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF
IN SUPPORT OF APPELLANT' APPEAL
TO THE BOARD OF PATENT APPEALS

Applicant (hereafter "Appellant") hereby submits this Brief in support of an Appeal from a decision of a Final Office Action mailed August 22, 2005, and sustained in an Advisory Action mailed November 7, 2005, in the above-referenced case. Appellant respectfully requests consideration of this appeal by the Board of Patent Appeals for allowance of the invention as presently recited in the claims.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest of the above-referenced U.S. Patent application is Intel Corporation of 2200 Mission College Boulevard, Santa Clara, California 95052, to whom the application has been assigned.

II. RELATED PROCEEDINGS

To the best of Appellant's knowledge, there are no prior or pending appeals, interferences, or judicial proceedings related to the subject matter of this appeal that will directly affect, be directly affected by, or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF THE CLAIMS

Claims 9, 20, 31, and 42 have been canceled.

Claims 1-8, 10-19, 21-30, 32-41, and 43-44 are pending in the above-referenced application, and were finally rejected in the Final Office Action mailed August 22, 2005. Appellant is cognizant of the new policy that puts claims directed to propagated signals in disfavor. Thus, Appellant respectfully requests that claims 23-30 and 32-33 be withdrawn from consideration in this Appeal. Therefore, claims 1-8, 10-19, 21-22, 34-41, and 43-44 are the subject of this appeal.

IV. STATUS OF AMENDMENTS

In response to the Final Office Action mailed August 22, 2005 rejecting the above-referenced claims, Appellant filed an Amendment After Final on October 24, 2005, after which the November 7, 2005 Advisory Action was sent. Appellant then filed a Notice of Appeal on December 22, 2005. A copy of all claims on appeal is attached hereto as Appendix A.

V. SUMMARY OF THE INVENTION

A device driver receives a network packet having a corresponding security association (SA). See [0018], [0020]. The packet may be an ingress or egress packet. See [0019]. The packet has a key value with which to locate the corresponding SA. See [0020]. If the packet is an ingress packet, the key value is hashed to determine a location of the SA in an ingress lookup table. See [0023], [0029]. If the packet is an egress packet, the key value is hashed to determine a location of the SA in an egress lookup table. See [0021], [0023], [0029]. Thus, SA information is stored in separate tables, in contrast to what has been previously done. See [0019], [0022].

The ingress and egress tables have information about the SA. See [0023]. The lookup tables can include an index to a location of the SA in memory, and the SA information can then be retrieved from memory. See [0027].

VI. GROUNDS OF REJECTION

Claims 1-8, 10-19, 21-30, 32-41, and 43-44 stand rejected under 35 U.S.C. § 103(a) as being unpatentable for obviousness over U.S. Patent No. 6,505,192 of Godwin (hereinafter "Godwin") in view of U.S. Patent No. 6,763,394 of Tuck, III et al. (hereinafter "Tuck"), and further in view of a webpage based upon an article "Monitoring Ethernet Network Activity with NDIS Drivers" of Apparna et al. (hereinafter "Apparna").

VII. ARGUMENT

Of the rejected claims for consideration in this Appeal, claims 1, 12, and 34 are independent claims, with the other claims depending either directly or indirectly from the independent claims.

Appellant maintains that the Office Actions have failed to set forth a prima facie case of obviousness under MPEP § 2143 at least for failing to set forth each and every element of the claimed invention. The cited references fail to support an obviousness rejection of the claims at least because they fail to set forth at least one element of the invention as recited in the independent claims. Additionally, Applicant submits that the references are not properly combinable to support the assertions made in the Office Actions.

A. Improper Combination of References

Regarding the combination of the references, Applicant stated in the Response to the Final OA that the rejection is based upon impermissible hindsight, using Applicant's application as a reconstructive guide to suggest the combination of the elements from the various references. Applicant submits that one skilled in the art would **not** have looked to combine the references as set forth in the Final Office Action.

Regarding the references themselves, as Applicant has understood the references:

Godwin discusses using a pseudo-connection memory block to store address and port information for packets to reduce search time for this information. In this way information can be cached and searched. See Abstract; col. 2, line 29 to col. 4, line 67.

Tuck discusses determining in a network router whether to pass packets from an ingress port to an egress port, or whether to drop the packets. See Abstract. Thus, the discussion of ingress and egress pass/drop lookups being made separately is made only in reference to a network router, and has no application to packets received at a device driver. Furthermore, the reference discusses pass and drop lookups within the router, and fails to disclose or suggest the association of a security association with the packets. Significantly, the reference discusses only determining whether packets in one part of the router will be dropped or passed to another part of the same router. The "rules" mentioned by the reference are only mentioned in terms of rules for determining whether to pass or drop a packet. See col. 2, lines 52 to 67. The rules do not relate to the application of cryptographic operations on a packet, as would be understood by one skilled in the art through the use of the term "security association." Thus, significantly, the teachings of Tuck are not at all related to security associations, or the retrieving of security association information for packets. The Office Actions fail to make any attempt to provide reasoning as to why a discussion of a determination to pass or drop a packet from one part of a router to another would have any application to either: 1) the discussion of Godwin regarding storing address and port information for packets, or, 2) storing security associations as recited in the claimed invention. The Advisory Action merely states that both references determine whether to drop packets and so they are combinable. Whether or not the discussion of Godwin is applicable to the claimed invention, the discussion of Tuck is wholly inapplicable to the problem resolved by the claimed invention; therefore, there is no motivation to combine the references. See MPEP 2143.01.

Applying the above discussion to the specifics of the Office Actions, Appellant notes that the Office Actions rely on Tuck at col. 5, lines 28 to 38 as motivation to use multiple rather than a single table. The part of the reference relied on in the Office Actions provides no motivation to split ingress and egress tables of SAs as recited in the claims. Rather, the section relied on refers to having tables of rules for whether to drop a packet on ingress or on egress. The relied-upon section further specifically states that the rules are "often independent," and therefore space would be wasted by using a single table instead of separate tables. This is directly in contrast to the use of separate tables as described in the Specification of the patent application that is the subject of this Appeal. In the Specification, it is explained that the use of separate SA tables generally requires more memory than using a single memory. Thus, the reference teaches away

from combining the references to solve the problem addressed by the claimed invention. Appellant points out that the same SA is applicable to processing of a packet on ingress **and** egress, which is in contrast to the rules of Tuck.

Regarding Apparna, the reference refers to a network device driver, and specifically to NDIS. No mention is given within Apparna regarding how to process packets, the use of security associations, and/or the storing of security associations in tables. Apparna is a general overview of what a device driver is, provides a few specifics as to its application or use, and fails to cure the deficiencies of the references mentioned above. Thus, contrary to the assertion in the Final Office Action at pages 3 to 4, no reason is either expressly or implicitly provided within the references that would suggest using a device driver to implement the method of Godwin, and certainly not Tuck (which occurs within a network switch, as explained above). Neither the references nor the Office Actions provide any suggestion as to how the method of Godwin regarding storing of pseudo-connection address information, nor the method of Tuck regarding a switch for determining whether to pass or drop a packet from an ingress port to an egress port, would be desired to be applied in a device driver. Nor do the references or the Office Actions set forth any reasoning to suggest how such methods of Godwin or Tuck could be accomplished by a device driver, nor why these techniques would supposedly apply to a device driver.

Therefore, there is no motivation to combine the references. Appellant submits that the only way to reach the conclusions in the Final Office Action is through the use of impermissible hindsight. The Final Office Action has therefore fails to set forth a prima facie case of obviousness of the independent claims under MPEP §§ 2142-2143, at least for failing to set forth a properly combinable set of references. The combination of references used to reject the claims in the Final Office Action results from improper hindsight, and not from the application of knowledge of those skilled in the art at the time of the invention

B. <u>Improper Application of the References to the Claimed Invention</u>

Even assuming that the references were properly combinable, which Appellant maintains would be improper, as discussed above, the references fail to support the rejection set forth in the Office Actions. The Office Actions have failed to provide reasoning as to why application of rules on whether to drop packets is asserted to be applicable to the obtaining of an appropriate SA to apply to a packet as recited in the claimed invention. Appellant maintains that the

references are not applicable to the subject matter of the claimed invention, and the interpretations made in the Office Actions are not supported.

The Office Actions acknowledge that Godwin fails to disclose or suggest at least one of the elements of the claimed invention. In particular, Godwin fails to suggest separate ingress and egress tables for SAs. Appellant adds that Godwin fails to mention the desirability of changing the traditional methods of searching SA tables. See, e.g., col. 6, lines 47 to 65. Through the discussion above, the attentive reader will see that Tuck and Apparna fail to cure the admitted deficiencies of Godwin. Tuck fails to disclose or suggest SAs, and specifically fails to disclose or suggest storing SAs in separate tables for ingress and egress. The separation of the rules tables suggested in Tuck fails to suggest to one of skill in the art that SA tables can be separated, or even that it may be desirable to separate the tables. Apparna is not cited as curing these deficiencies, nor indeed does the reference cure the deficiencies pointed out above.

Whether alone or in combination, the cited references fail to disclose or suggest at least one element of the claimed invention, and so fail to support a prima facie case of obviousness under MPEP § 2143. Therefore, the independent claims are nonobvious over the primary references. As per MPEP §2143.03, claims depending from nonobvious independent claims are likewise nonobvious. Therefore, Applicant submits that the cited references fail to render obvious the invention as recited in the pending claims.

VIII. CONCLUSION

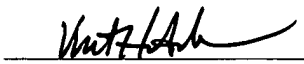
Appellant respectfully submit that all appealed claims in this application are patentable and request that the Board of Patent Appeals and Interferences overrule the Examiner and direct allowance of the rejected claims.

A single copy of this brief is submitted as per 37 C.F.R. §41.37(a), along with a check for $500.00 to cover the appeal fee for one other than a small entity as specified in 37 C.F.R. §1.17(c). Please charge any shortages and credit any overcharges to our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP

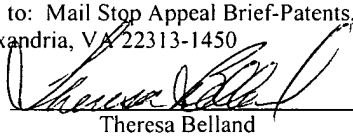
Date: February 28, 2006



Vincent H. Anderson
Reg. No. 54,962

12400 Wilshire Blvd., 7th Floor
Los Angeles, CA 90025-1026
Telephone: (503) 439-8778

I hereby certify that this correspondence is being deposited with the United States Postal service as first class mail on the below date with sufficient postage in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450 Alexandria, VA 22313-1450

Signature  2/28/06

Theresa Belland Date

APPENDIX A: CLAIMS ON APPEAL

1. (Previously Presented) A method comprising:

receiving at a device driver a network packet having a corresponding security association (SA);

determining if the packet is an ingress packet or an egress packet;

determining for the packet a key value corresponding to the SA;

if the packet is an ingress packet, hashing the key value to determine a location of an entry in an ingress lookup table, and if the packet is an egress packet, hashing the key value to determine a location of an entry in an egress lookup table, the entry in the ingress lookup table and the entry in the egress lookup table containing information corresponding to the SA, the ingress lookup table being a separate lookup table from the egress lookup table;

retrieving from the entry an index to a location of the SA in memory; and

retrieving the SA from memory based on the index.

2. (Previously Presented) The method of claim 1 wherein receiving the network packet comprises the device driver being passed an egress packet from an electronic system operating system.

3. (Previously Presented) The method of claim 1 wherein receiving the network packet comprises the device driver being passed an ingress packet from a network interface device.

4. (Original) The method of claim 1 wherein the key value is a handle created for the SA for an egress packet.

5. (Original) The method of claim 1 wherein the key value is a security parameter index (SPI) extracted from the packet for an ingress packet.

6. (Original) The method of claim 1 wherein the lookup table entry comprises the key value and the index.

7. (Original) The method of claim 6 wherein the lookup table entry further comprises a counter to track collisions for the entry.

8. (Previously Presented) The method of claim 1 further comprising the location in memory of an SA corresponding to egress traffic being in a first table, and the location in memory of an SA corresponding to ingress traffic being in a second table, the tables being separate tables in memory.

9. (Canceled)

10. (Original) The method of claim 1 further comprising supporting a number of network traffic streams, wherein the lookup table has 2^N entries, where N is an integer, 2^N being the lowest binary number greater than five times the number of network traffic streams supported.

11. (Previously Presented) The method of claim 1 wherein hashing the key value comprises using a bit-wise AND hash function with a mask of value 2^N-1, where N is an integer, wherein the hash table contains 2^N entries.

12. (Previously Presented) An article comprising a machine-accessible medium to provide content to cause one or more electronic systems to:

receive at a device driver a network packet having a corresponding security association (SA);

determine if the packet is an ingress packet or an egress packet;

determine for the packet a key value corresponding to the SA;

if the packet is an ingress packet, hash the key value to determine a location of an entry in an ingress lookup table, and if the packet is an egress packet, hash the key value to determine a location of an entry in an egress lookup table, the entry in the ingress lookup table and the entry in the egress lookup table containing information corresponding to the SA, the ingress lookup table being a separate lookup table from the egress lookup table;

retrieve from the entry an index to a location of the SA in memory; and

retrieve the SA from memory based on the index.

13. (Previously Presented) The article of claim 12 wherein to receive the network packet comprises the device driver to be passed an egress packet from an electronic system operating system.

14. (Previously Presented) The article of claim 12 wherein to receive the network packet comprises the device driver to be passed an ingress packet from a network interface device.

15. (Original) The article of claim 12 wherein the key value is a handle created for the SA for an egress packet.

16. (Original) The article of claim 12 wherein the key value is a security parameter index (SPI) extracted from the packet for an ingress packet.

17. (Original) The article of claim 12 wherein the lookup table entry comprises the key value and the index.

18. (Original) The article of claim 17 wherein the lookup table entry further comprises a counter to track collisions for the entry.

19. (Previously Presented) The article of claim 12 further comprising the location in memory of an SA corresponding to egress traffic being in a first table, and the location in memory of an SA corresponding to ingress traffic being in a second table, the tables being separate tables in memory.

20. (Canceled)

21. (Original) The article of claim 12 further comprising to support a number of network traffic streams, wherein the lookup table has 2^N entries, where N is an integer, 2^N being the lowest binary number greater than five times the number of network traffic streams supported.

22. (Previously Presented) The article of claim 12 wherein to hash the key value comprises using a bit-wise AND hash function with a mask of value 2^N-1, where N is an integer, wherein the hash table contains 2^N entries.

23. (Withdrawn) An electronic data signal embodied in a data communications medium shared among a plurality of network devices comprising content to cause one or more electronic systems to:

receive at a device driver a network packet having a corresponding security association (SA);

determine if the packet is an ingress packet or an egress packet;

determine for the packet a key value corresponding to the SA;

if the packet is an ingress packet, hash the key value to determine a location of an entry in an ingress lookup table, and if the packet is an egress packet, hash the key value to determine a location of an entry in an egress lookup table, the entry in the ingress lookup table and the entry in the egress lookup table containing information corresponding to the SA, the ingress lookup table being a separate lookup table from the egress lookup table;

retrieve from the entry an index to a location of the SA in memory; and

retrieve the SA from memory based on the index.

24. (Withdrawn) The electronic data signal of claim 23 wherein to receive the network packet comprises the device driver to be passed an egress packet from an electronic system operating system.

25. (Withdrawn) The electronic data signal of claim 23 wherein to receive the network packet comprises the device driver to be passed an ingress packet from a network interface device.

26. (Original) The electronic data signal of claim 23 wherein the key value is a handle created for the SA for an egress packet.

27. (Original) The electronic data signal of claim 23 wherein the key value is a security parameter index (SPI) extracted from the packet for an ingress packet.

28. (Original) The electronic data signal of claim 23 wherein the lookup table entry comprises the key value and the index.

29. (Original) The electronic data signal of claim 28 wherein the lookup table entry further comprises a counter to track collisions for the entry.

30. (Withdrawn) The electronic data signal of claim 23 further comprising the location in memory of an SA corresponding to egress traffic being in a first table, and the location in memory of an SA corresponding to ingress traffic being in a second table, the tables being separate tables in memory.

31. (Canceled)

32. (Withdrawn) The electronic data signal of claim 23 further comprising to support a number of network traffic streams, wherein the lookup table has 2^N entries, where N is an integer, 2^N being the lowest binary number greater than five times the number of network traffic streams supported.

33. (Withdrawn) The electronic data signal of claim 23 wherein to hash the key value comprises using a bit-wise AND hash function with a mask of value 2^N-1, where N is an integer, wherein the hash table contains 2^N entries.

34. (Previously Presented) An electronic system comprising:

one or more processors;

a network interface coupled with the one or more processors to provide a communications path between the electronic system and a network, the network interface to have a corresponding device driver to be executed on one or more of the processors; and

a memory coupled with the one or more processors, the memory to have a program to provide instructions for the electronic system to receive at the device driver a network packet having a corresponding security association (SA), the program to determine if the packet is an

ingress packet or an egress packet, to determine for the packet a key value corresponding to the SA, and if the packet is an ingress packet, hash the key value to determine a location of an entry in an ingress lookup table, and if the packet is an egress packet, hash the key value to determine a location of an entry in an egress lookup table, the entry in the ingress lookup table and the entry in the egress lookup table containing information corresponding to the SA, the ingress lookup table being a separate lookup table from the egress lookup table, to retrieve from the entry an index to a location of the SA in memory, and to retrieve the SA from memory based on the index.

35. (Previously Presented) The electronic system of claim 34 wherein the program to receive the network packet comprises the device driver to be passed an egress packet from an operating system.

36. (Previously Presented) The electronic system of claim 34 wherein the program to receive the network packet comprises the device driver to be passed an ingress packet from the network interface.

37. (Original) The electronic system of claim 34 wherein the key value is a handle created for the SA for an egress packet.

38. (Original) The electronic system of claim 34 wherein the key value is a security parameter index (SPI) extracted from the packet for an ingress packet.

39. (Original) The electronic system of claim 34 wherein the lookup table entry comprises the key value and the index.

40. (Original) The electronic system of claim 39 wherein the lookup table entry further comprises a counter to track collisions for the entry.

41. (Previously Presented) The electronic system of claim 34 further comprising the location in memory of an SA corresponding to egress traffic being in a first table, and the location in memory of an SA corresponding to ingress traffic being in a second table, the tables being separate tables in memory.

42. (Canceled)

43. (Original) The electronic system of claim 34 further comprising the program to support a number of network traffic streams, wherein the lookup table has 2^N entries, where N is an integer, 2^N being the lowest binary number greater than five times the number of network traffic streams supported.

44. (Previously Presented) The electronic system of claim 34 wherein to hash the key value comprises using a bit-wise AND hash function with a mask of value 2^N-1, where N is an integer, wherein the hash table contains 2^N entries.